UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,697	03/31/2000	Michael F. Angelo	COMP:0061	3660

7590 03/08/2004

Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	4

DATE MAILED: 03/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/540,697	ANGELO ET AL.	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-55 are rejected under 35 U.S.C. 102(b) as being anticipated by Mattison (US 5,778, 070).

a. *Referring to claim 1:*

i. Mattison teaches:

(1) a first section of non-volatile memory configured to store a BIOS program, the first section of non-volatile memory being reprogrammable **[i.e., the BIOS is stored in flash memory to allow for field updates and reprogramming of the BIOS (column 1, lines 56-57). In fact, referring to Figure 2, typically the upper 64 kilobytes in the first megabyte of the original PC architecture is allocated for BIOS (column 7, lines 21-23)]**; and

(2) a second section of non-volatile memory operatively coupled to the first section of non-volatile memory, the second section of non-volatile memory being configured to store a boot-block program **[i.e., referring to Figure 2, "a boot-block program" is considered to also store in a flash memory 108 (column 5, line 55) and any extensions to the BIOS is contained in a region below the 64 kilobytes allocated to the BIOS, along with any other "program memory", in which a boot-block program is inherently provided (column 7, lines 23-25)]**;

(3) the boot-block program having a first validation routine configured to validate the BIOS program stored in the first section of non-volatile memory, and the BIOS program having a second validation routine configured to validate the boot-block program stored in the second section of non-volatile memory

[i.e., referring to Figure 3, in block 308, the current program in flash memory 108 is for verifying and/or validating the source and content of the flash memory upgrade program, whereby "a first validation routine configured to validate the BIOS program and a second validation routine configured to validate the boot-block program" are considered to include in this part of the upgrade program (column 9 lines 38-40)].

b. *Referring to claim 2:*

i. Mattison further teaches:

(1) wherein the first section of non-volatile memory comprises a protected segment of a reprogrammable memory device **[i.e., because the BIOS is the first program to gain control of the processor after reset, it is critical to any security scheme. Therefore, the BIOS must be protected from modification during any time where the machine is in an unsecured operating mode, especially in cases where the BIOS is stored in flash memory. The BIOS is stored in flash memory to allow for field updates and reprogramming of the BIOS (column 1, lines 50-57)]**.

c. *Referring to claim 3:*

i. Mattison further teaches:

(1) wherein the second section of non-volatile memory comprises a reprogrammable segment of the reprogrammable memory device **[i.e., any extensions to the BIOS is contained in a region below the 64 kilobytes allocated to the BIOS, that is "the second section", along with any other "program memory" (column 7, lines 23-25)]**.

d. *Referring to claim 4:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above

e. *Referring to claim 5:*

i. Mattison further teaches:

(1) wherein the first section of non-volatile memory comprises a first memory device **[i.e., referring to Figure 2, "a first memory device " is considered to include in a flash memory 108].**

f. *Referring to claim 6:*

i. Mattison further teaches:

(1) wherein the second section of non-volatile memory comprises a second memory device **[i.e., referring to Figure 2, "a second memory device" is considered to include in a flash memory 108].**

g. *Referring to claims 7-10:*

i. Mattison further teaches:

(1) wherein the boot-block program comprises a public key and a hash algorithm used to validate the BIOS program; wherein one of the boot-block program and the BIOS program comprises an encrypted hash correlative to the BIOS program; wherein the encrypted hash is encrypted using a private key correlative to the public key; wherein the boot-block program validates the BIOS program by calculating a first hash of the BIOS program using the hash algorithm, using the public key to decrypt the encrypted hash to produce a second hash, and comparing the first hash to the second hash **[i.e., Figure 3 shows a series of operations for reprogramming flash memory 108. In block 302, a flash memory upgrade program containing a new flash memory image (e.g., a new BIOS image) for flash memory 108 (containing the current BIOS) would be loaded into system memory 106 and executed. The flash memory upgrade program would incorporate a digital signature which is "signed" by the private key of the vendor; the digital signature being the original hash value of the flash memory upgrade program after the original hash value has been encrypted with the vendor's private key. Operation would then continue with block 304. In block 304, after the flash memory upgrade program begins execution, the flash memory upgrade program would call a special function in the current program contained in flash memory 108, requesting to install the new flash memory image. This call would specify the address and size of the flash memory upgrade program located in system**

memory 106. Therefore, when the flash memory upgrade program (containing the new BIOS image) begins execution, it transfers control to the program contained in flash memory 108 (the current BIOS), requesting to update the current BIOS, that is "to validate the BIOS program" (column 7, lines 64-67 through column 8, lines 1-20)].

h. *Referring to claims 11-15:*

i. Mattison further teaches:

(1) wherein the boot-block program does not allow the system to boot if the first hash does not match the second hash, and wherein the boot block program does allow the system to boot if the first hash matches the second hash; wherein the system warns a user if the first hash does not match the second hash; wherein the boot-block program allows the system to boot if the first hash does not match the second hash; wherein the boot-block program allows the system to boot if the first hash does not match the second hash in response to an instruction to boot from the user; wherein various system resources are enabled or disabled depending upon whether the first hash matches the second hash **[i.e.., In block 308, the current program in flash memory 108 would then verify the source and content of the flash memory upgrade program (which includes the new flash memory image) by: (a) decrypting the digital signature using the vendor's public key stored in the current program to obtain the original hash value; (b) independently calculating a hash value for the flash memory upgrade program which is resident in main system memory; and (c) comparing the original hash value obtained from decrypting the digital signature with the independently generated hash value to find a match. If the hash values match, indicating that the flash memory upgrade program contained in main memory originated from the authorized creator AND has not been modified, then operation will continue with block 310. If the hash value does not match, the upgrade will be aborted. In an alternate embodiment, the user can be notified of the failed upgrade in another step (not shown), whereby the routine for allowing to boot up the system is inherently provided in the flash memory upgrade program (column 9, lines 38-58)].**

i. *Referring to claims 16-19:*

i. These claims have limitations that is similar to those of claims 7-10, thus they are rejected with the same rationale applied against claims 7-10 above.

j. *Referring to claims 20-24:*

i. These claims have limitations that is similar to those of claims 11-15, thus they are rejected with the same rationale applied against claims 11-15 above.

k. *Referring to claim 25:*

i. Mattison further teaches:

(1) CMOS memory operatively coupled to at least one of the first section of non-volatile memory and the second section of non-volatile memory **[i.e., referring to Figure 2, "CMOS memory" is considered to include in system memory which couples to flash memory 108, that is "a non-volatile memory"]**; and

(2) non-volatile random access memory (NVRAM) operatively coupled to at least one of the first section of non-volatile memory and the second section of non-volatile memory **[i.e., referring to Figure 2, "non-volatile random access memory (NVRAM) operatively coupled to at least one of the first section of non-volatile memory and the second section of non-volatile memory at least one of the first section of non-volatile memory and the second section of non-volatile memory" is considered to include in flash memory 108].**

l. *Referring to claims 26 and 27:*

i. Mattison further teaches:

(1) wherein the first validation routine is configured to validate at least one of the CMOS memory and the NVRAM; wherein the second validation routine is configured to validate at least one of the CMOS memory and the NVRAM **[i.e., referring to Figures 2 and 3, in block 308, the current program in flash memory 108 is for verifying and/or validating the source and content of the flash memory upgrade program, in which the "the first validation routine is configured to validate at least one of the CMOS memory and the NVRAM and the**

second validation routine is configured to validate at least one of the CMOS memory and the NVRAM" is considered to be part of the flash memory upgrade program routine (column 9 lines 38-40)].

m. *Referring to claim 28:*

i. Mattison further teaches:

(1) comprising a processing system operatively coupled to the first section of non-volatile memory and to the second section of non-volatile memory **[i.e., referring to Figure 2, a system memory controller is included which provides a mode where the processor is restricted to accessing only the flash memory, which includes "the first section of non-volatile memory and to the second section of non-volatile memory" (i.e., a mode where the processor can only execute instructions from the flash memory and not from any other memory such as a main system memory or cache) (column 2, lines 58-63)].**

n. *Referring to claims 29 and 42:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

o. *Referring to claims 30, 36, 43, and 49:*

i. These claims have limitations that is similar to those of claims 7-10, thus they are rejected with the same rationale applied against claims 7-10 above.

p. *Referring to claims 31-35, 37-41, 44-48, and 50-54:*

i. These claims have limitations that is similar to those of claims 11-15, thus they are rejected with the same rationale applied against claims 11-15 above.

q. *Referring to claim 55:*

i. Mattison further teaches:

(1) performing at least one of a self-correcting, reset, and default function if the first hash does not match the second hash **[i.e., the BIOS first performs a Power On Self Test (POST), in which all the system hardware units (such as the interrupt controller, the Direct Memory Access (DMA) controller, and**

timers/counters) are tested and programmed for normal operation, wherein "a self-correcting, reset, and default function if the first hash does not match the second hash" is considered to perform using this same Power On Self Test (POST) (column 1, lines 16-20)].

3. Claims 1, 29, 30, 36, 42, 43, and 49 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis (US 5,844, 986).

a. *Referring to claim 1:*

i. Davis teaches:

(1) a first section of non-volatile memory configured to store a BIOS program, the first section of non-volatile memory being reprogrammable **[i.e., referring to Figure 1, the boot-up program 43 is stored within non-volatile memory 42 (column 3, lines 18-19)]**; and

(2) a second section of non-volatile memory operatively coupled to the first section of non-volatile memory, the second section of non-volatile memory being configured to store a boot-block program **[i.e., referring to Figure 1, "a boot-block program" is considered to also store in a non-volatile memory 42];**

(3) the boot-block program having a first validation routine configured to validate the BIOS program stored in the first section of non-volatile memory, and the BIOS program having a second validation routine configured to validate the boot-block program stored in the second section of non-volatile memory **[i.e., the primary focus of Davis' invention, therefore, is to prevent corrupting the BIOS by a computer virus. This is achieved by imposing an authentication and validation procedure before the contents of the BIOS flash memory are modified, whereby "a first validation routine configured to validate the BIOS program and a second validation routine configured to validate the boot-block program" are considered to include in this part of the validation procedure (column 1, lines 63-67)].**

b. *Referring to claim 29:*

i. Davis teaches:

(1) means for validating a BIOS program stored in a first section of non-volatile memory **[i.e., the authentication and validation are performed by a security processor which contains the BIOS firmware. One example of such a security processor is a cryptographic coprocessor. The cryptographic processor authenticates and validates the BIOS firmware by using secret information such as a digital signature embedded in the BIOS upgrade (column 2, lines 58-63)]**;

(2) means for validating a boot-block program stored in a second section of non-volatile memory **[i.e., referring to Figure 1, the cryptographic processor, that is also for "validating a boot-block program stored in a second section of non-volatile memory"]**.

c. *Referring to claims 30, 36, 43, and 49:*

i. Davis further teaches:

(1) means for storing a public key and a hash algorithm used to validate the BIOS program; means for storing an encrypted hash correlative to the BIOS program; means for calculating a first hash of the BIOS program using the hash algorithm; means for decrypting the encrypted hash using the public key to produce a second hash; and means for comparing the first hash to the second hash **[i.e., referring to Figure 1, a cryptographic coprocessor 34, including a non-volatile memory 42, that is for "storing a public key and a hash algorithm used to validate the BIOS program and storing an encrypted hash correlative to the BIOS program" and a processing unit 41, that is for "decrypting the encrypted hash using the public key to produce a second hash and comparing the first hash to the second hash"]**.

d. *Referring to claim 42:*

i. This claim has limitations that is similar to those of claim 29, thus it is rejected with the same rationale applied against claim 29 above.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 11, 20, 31, 37, 44, and 50 are alternatively rejected under 35 U.S.C. 103(a) as being unpatentable over Mattison (US 5, 778, 070) as applied to claim 11 in paragraph 2 above, and further in view of Davis et al (US 6, 401, 208 B2).

a. *Referring to claims 11, 20, 31, 37, 44, and 50:*

i. Assuming *arguendo* that Mattison does not really point out:

(1) wherein the boot-block program does not allow the system to boot if the first hash does not match the second hash, and wherein the boot block program does allow the system to boot if the first hash matches the second hash;

ii. Davis, however, teaches:

(1) Concurrent or subsequent to this data transfer, within the cryptographic device, the BIOS certificate is decrypted using the root certification key (block 660). This operation is performed to retrieve a public key of the signatory of the BIOS signature (e.g., BIOS vendor). Then, the preloaded digest signature is decrypted using the public key of the BIOS vendor, for example, to recover a pre-loaded digest (block 665). After recovering the pre-loaded digest, the BIOS code is read and undergoes the one-way hash function to produce a resultant digest (block 670). The resultant digest is compared to the pre-loaded digest (block 675). If no match occurs, the host processor is precluded from continuing its boot procedure (blocks 680 and 685). However, if there is a match, the BIOS code has been authenticated as valid, which permits the host processor to execute the software code, that means continuing its boot procedure **(column 5, lines 66-67 through column 6, lines 1-13).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) utilize the booting procedure of Mattison with the cryptographic device to authenticate software code, loaded into the cryptographic device during a boot procedure, before permitting the host processor to execute the software code **(column 1, lines 64-67 of Davis).**

iv. The ordinary skilled person would have been motivated to:

(1) utilize the booting procedure of Mattison with the cryptographic device for the necessity in providing a protected environment for execution of code and for manipulation of data within a computer **(column 1, lines 58-60 of Davis).**

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Miller (US 6, 308, 265) discloses an apparatus and a method for protecting boot block code while allowing updating to BIOS code during a flash BIOS operation. The boot block code is stored in a boot block or boot region of a flash part, and then a copy of the boot block code is written into another region of the flash part (see abstract).

b. Albrecht et al (US 6, 510, 521 B1) discloses an electronic signature is generated in a predetermined manner and attached to a transferable unit of write data, to facilitate authenticating the write data before allowing the write data to be written into a protected non-volatile storage. The write data is authenticated using a collection of secured authentication functions. Additionally, the actual writing of the authenticated write data into the protected non-volatile storage is performed by a secured copy utility (see abstract).

c. Hasbun (US 6, 205, 548 B1) discloses Code is written to a selected portion of a nonvolatile memory having a first portion associated with a first range of addresses and a second portion associated with a second range of addresses, wherein the selected portion is the second portion (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
March 1, 2004